Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Hybrid Cubes Certificate Encryption Revocation with Capability for Mobile Ad Hoc Networks

D. Megala*, Aruna Devi .P
Assistant Professor
Department of Computer Technology Department of Computer Technology
Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, India

Abstract—Development and assessment of the secure in the Mobile Adhoc networks (MANET) for real time applications makes several numbers of the attacks problems during data transmission. It becomes more motivated area for several numbers of researches to study the impact of security problem during the development stage of MANET. In order to meet this type of the problems in MANET, in this work propose a novel security schema along with certificate revocation during data transmission process. The generation of the key values for each user for each certificate plays major important role to perform this process in this work presents a novel hybrid cubes certificate encryption (HCCE) scheme is proposed in this work for security in MANET. To enhance the security of the schema the reliability of the organization is proposed to formulate warned nodes and normal nodes before recovering them. The experimentation results of the proposed HCCE scheme are evaluated by simulation analysis. It shows that the proposed certificate revocation scheme is successful and well-organized to assurance secure communications in mobile ad hoc networks.

Keywords— Mobile ad hoc networks (MANETs), Certificate Revocation, security, threshold, encryption, Hybrid Cubes Certificate Encryption (HCCE).

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have been used in several areas in recent years or earlier work because of their mobility, self-motivated topology, and ease of operation. Securing of MANET be supposed to become a major challenge and it is enormously considerable to assess secure MANET software in real time applications. The real time security system in the MANET includes the following four major steps (Fig.1). Primary, should realize application aim since the final examination of achievement used for a safe MANET is how fine the MANET application attain its considered operation goal in spite of threats and attacks. This helps us plan experimentation, together with the alternative of test cases and valuation models. In third stage of the process, require a come up through a set of suspiciously intended attack situation. A great deal like further testing in software engineering order, this must appear following a widespread analysis of the possible threats to MANET objectives and the set of test cases must cover these threats expansively. Methodical approaches approximating attack categorization [1] second-hand in protected MANET test case progress.

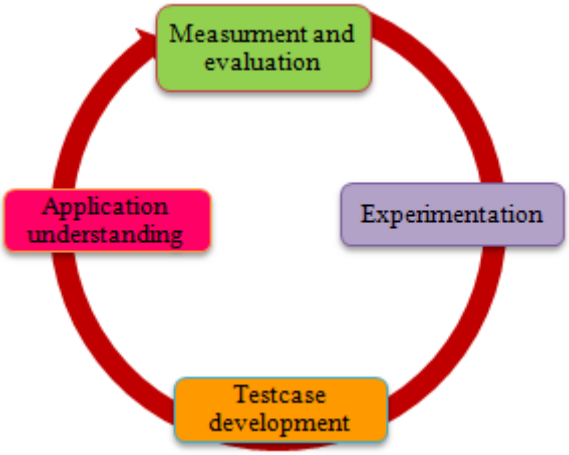

Fig. 1. The Circle of Securing MANET

Securing of MANET be supposed to become a major challenge for these network services. Make use of security [2-3] is so of most important in MANET networks. Provisioning confined transmission communications among mobile nodes in an aggressive situation caused by malicious attacker to interrupt network security in MANETs. Certificate management is an extensively second-hand method which provide as a means of transmission confidence in a public key

communications [4] to safe network services. An absolute safety resolution designed for certificate managing must include three major parts: prevention, detection, and revocation. Several number of research work have been done in these areas, such as certificate distribution [5], attack detection [6-7], and certificate revocation [8-9]. Certification is a necessity to safe network transmission communications. It is embodied as a information formation in which the public key is generated to each attribute by using digital signature algorithm , and can be second-hand to confirm with the intention of a public key be in the right place to an character and to thwart corrupting attacks in MANET.

Several number of the research has been done to detect the malicious attacks from MANET. Some of the other type of the attacks in the network also identified in earlier work as earlier as possible. Among them all of the methods in the network one of the most important method certificate revocations plays major important role and eliminate the certificate of nodes if the specific node is identified is as attacker node. If the specific node is found as misbehaved node then the selected node is removed from MANET, their activities of the nodes are also stopped instantaneously. The major aim of the research work is to solve the problem of the network security based on the creation of the certificate authority that provides more security in MANETs to confirm the authenticity of the user, to improve the security in this work proposed a hybrid cubes certificate encryption (HCCE) for MANET.

The entire procedure of the paper is organized as follows: Section 2, study the Background knowledge of existing certificate revocation techniques in MANETs, and analyze both advantages and disadvantages of these Schemes. Section 3 studies the procedure of the proposed hybrid cubes certificate encryption revocation that introduces the certificate revocation process. In Section 4 measure the performance evaluation of our scheme. Finally, conclude the paper in Section 5 and scope of the future work also mentioned.

.

II. BACKGROUND KNOWLEDGE

In earlier work MANET with security schema there are two categories of the schema was proposed such as voting and non-voting based schema. Voting based URSA scheme is developed by Luo et al [10] .It is to force out nodes of MANET which are hateful. Apprehension and revocation of the certificates are completed through the neighbors of lately joined nodes. In URSA, every one node exchanges were monitoring information each and every one the way through its neighbors which is discovered through one-hop monitoring. URSA is not capable to determine its issue in concentrate on false claim beginning the attacking nodes.

Arboit et al. [11] consent each and every one node in the network to choose mutually. It is different from URSA in the method nodes vote through variable weights. It is determined based on the parameters of dependability and honesty of the node determined from its past communication. And this facilitate in rising accurateness of credential revocation. In this each and every one node leads a high transportation overhead and larger revocation time.

A new method based in the security mechanism with certificate revocation is introduced in [12] through only one duration of time. Thus the condemning node is given up itself since its credential is also invalidated. The proposed certificate mechanism removes the number of attacker in the MANET through improving the security of the network. This mechanism decrease together time necessary to remove a node and interactions over head appropriate in the direction of its desperate strategy. But the major problem of the work the proposed methods doesn't identify the falsely nodes from malicious attackers ,it is also becomes major important issue ,so the results of the MANET becomes less accuracy and some of the attackers nodes still not identified. New certificate based revocation schema follows the clustering procedure [13]. Each node in the MANET is formed as cluster. The message send by user from source to destination node is managed by certificate authority where the accused node is stored in warning list (WL) and accuser node is stored in blacklist (BL), correspondingly. Through some particular neighboring node based results the malicious attacker node is invalidated. It furthermore deals through the concern of forged allegation with the intention of facilitate the falsely accused node to be present unconcerned from the BL through its cluster head (CH).

Comprehensive survey of the security design based on the trust is studied in [13-14]. To calculate trust assessment, the majority of this scheme makes use of information based on two categories .In the initial category of the information neighboring nodes information is collected from each node in the network and this can be completed through eavesdropping nodes. The remaining information is considered as second hand information. Trust-based voting mechanism with clustering scheme is introduced in [15]. It estimates the constancy of node all the way through calculate the neighbor alteration ratio and the remaining battery power. To select CHs through via the voting method based on the votes value.

III. PROPOSED HYBRID CUBES CERTIFICATE ENCRYPTION REVOCATION METHODOLOGY

In this paper presents a novel hybrid cubes based certificate encryption schema, before that we specified the details of the certificate revocation schema, and then introduce the hybrid cubes certification encryption procedure. To invalidate a malicious attacker's certificate three major important stages are followed in this work, these stages are accusing, verifying, and notifying. The certificate revocation process starts with identification of the malicious nodes and normal nodes to distinguish the attacks from normal nodes. For example, assume that M be the malicious attacker one hop data transmission to identify the normal and malicious nodes in the network, as shown in Fig. 2, the certificate revocation schema procedure is described in the following manner:

Step 1: Consider a B, C, D, and E is the neighboring nodes which are identified from the malicious node M.

Step 2: Each and every one of the node send as packet from source to destination based on the CA alongside M.

Step 3: According to the earliest established packet the CA hold B and minimum to WL and BL, correspondingly, following authenticate the authority of node B.

Step 4: The CA broadcast the revocation communication to each and every one nodes in the MANET.

Step 5: Nodes modify their local WL and BL correspondingly to invalidate M be the malicious attacker certificate.

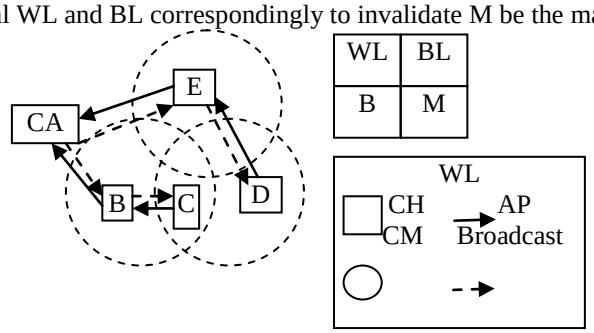

Fig. 2. Revoking a node's certificate

Accordingly, the probability with the intention of present are accurately m usual nodes (m individual a nonnegative integer, $m = (0, 1, 2, \dots)$ within the data communication area S along with attacker node, is equal to ,

$$Pr(m) = \frac{\lambda^m e^{-\lambda}}{m\,!} = \frac{(\theta\rho S)^M e^{-\theta\rho S}}{m\,!} \quad (1)$$

where ρ specifies density value for each nodes and θ is denoted as the total number of normal nodes in the network. As examined above, the total number of normal nodes is reduced. When $m = 0$ there is no usual nodes obtainable inside the attackers transmission range, their probability value is specified as ,

$$Pr(m = 0) = e^{-\theta\rho S} \quad (2)$$

From (2), the probability $Pr(m = 0)$ significantly enhance through the reduced density ρ; the effectiveness of distinguishing malicious attackers is considerably concentrated. Probability $Pr(m = 0)$ should be concentrated to promise a total number of normal nodes in the MANET to validate and normal nodes rapidly. The following principles are specified to calculate the threshold value for each certificate.

Policy 1: Minimizing False Release Probability: In the primary policy, make a decision K through probability $P_f(K)$ with N neighbors nodes. This probability $P_f(K)$ is calculated as follows:

$$P_f(K) = \sum_{i=K}^{N} \binom{N}{i} p^i (1-p)^{N-i} \quad (3)$$

Here, p specifies the probability value for each node with incorrectly discharging nodes beginning the WL based on threshold K.

Policy 2: Maximizing Correct Release Probability

In the second policy determine the probability $P_c(K)$ determination be effectively released from the WL.

$$P_c(K) = \sum_{i=K}^{N} \binom{N}{i} (1-p)^i p^{N-i} \quad (4)$$

where $(1 - p)$ denotes the probability value of each node take part in accurate accusation.

Policy 3: Maximizing Accuracy

Identify with the purpose of there is a substitution among the $P_f(K)$ and $P_c(K)$ way to find the value of the threshold K.

$$\gamma(K) = P_c(K) - P_f(K) \quad (5)$$

Hybrid cubes certificate encryption

Hybrid cubes certificate encryption methods follows the procedure of permutation integer value as major value to find the encryption key value based on Orthogonal Latin square to combine several number of information of nodes in balanced manner for Balanced Block Mixer. In this work there are n number of the cubes are present in Hybrid cubes certificate encryption Algorithm [16] . The transformation is achieve through varying the categorize of the sub-cubes through shifting , rotating rows and columns all along its cube plane. Conversely, permutation via straightforward mixture of row-shift and column-shift was established in the direction of exist fragile alongside Differential Chosen-Plaintext attack [17]. Based on this problem only motivate to perform improvement of compound permutation used for part of cipher propose. Granboulan et al [18] importance the necessitate designed for pseudo-random permutation with random set.

Encryption methods: Key schedule algorithm create secret keys and it becomes more important ,plays major part of role in the implementation of the cluster certificate based encryption schema and decryption procedure. Among them all of the procedure the procedure of encryption algorithm is illustrated in Fig. 3.

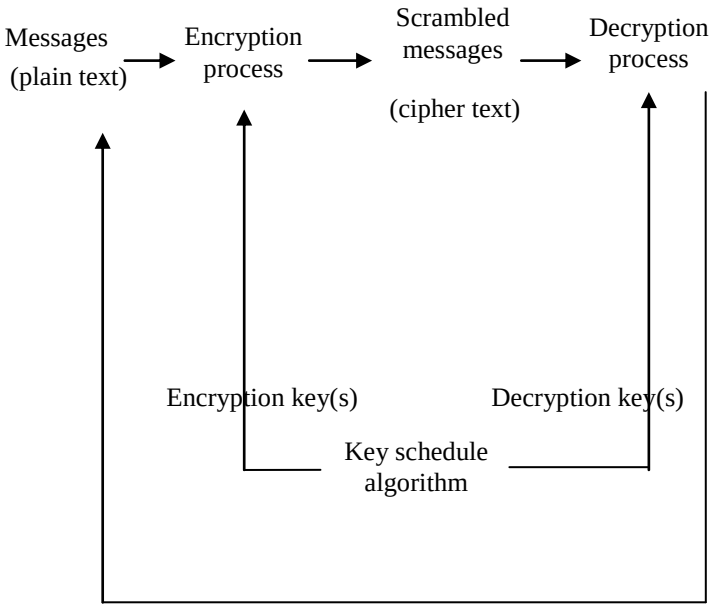

Fig 3. Basic Components of Symmetric Block Cipher

In this work the plaintext or original node information are encrypted using the secret key generated from key generation algorithm along with certificate authority for each node also maintained , the following possible number of bit value based on the keys such as 128-bit key , 192-bit and 256 -bit key are generated through potential key combination. The selected key bit value the data are encrypted and decrypted.

Decryption Process: it is same like as encryption except that the ciphertext information of each node is decrypted using decryption keys. It is performed based on the creation of confusion and diffusion procedure.

Kerchoffs's Principle: According to this principle, the strength of entire encryption and decryption procedure are measured. These principles ensure with the intention of they be no secret codes fixed through the unique designer of the cipher. In addition, cryptographic community is able to explicitly estimate the appropriateness of its basic arithmetical formulation.

IV. SIMULATION RESULTS

In this section, measure the performance accuracy of the proposed HHCE scheme and existing nonvoting, CCRVC schema, this procedure is implemented through the help of network simulator, Qualnet 4.0 [19]. To show the purpose of there is a substitution among the $P_f(K)$ and $P_c(K)$ way to find the value of the threshold K is compared with existing values and measure the results of the various K values . To estimate the accuracy of the proposed HHCE scheme, run simulation under various categories on the nodes and compare them with the existing schemes. The revocation time of the HHCE schema estimate the effectiveness and dependability of CR in the existence of malicious attacks. For each experiment of proposed HHCE scheme and existing nonvoting, CCRVC schema, obtain the average results from 50 simulation runs. Table 1 specifies the significant parameters second-hand in the simulation.

TABLE 1: SIMULATION PARAMETERS

Parameter	Value
Node placement	Uniform distribution
Mobility model	Random waypoint
Terrain dimensions	1000m *1000m
Transmission range	250m
Node speed	1m/2-10m/s
CH chosen probability ,R	0.3
Cluster update interval	20s
Voting time period	10s
Simulation time	600s

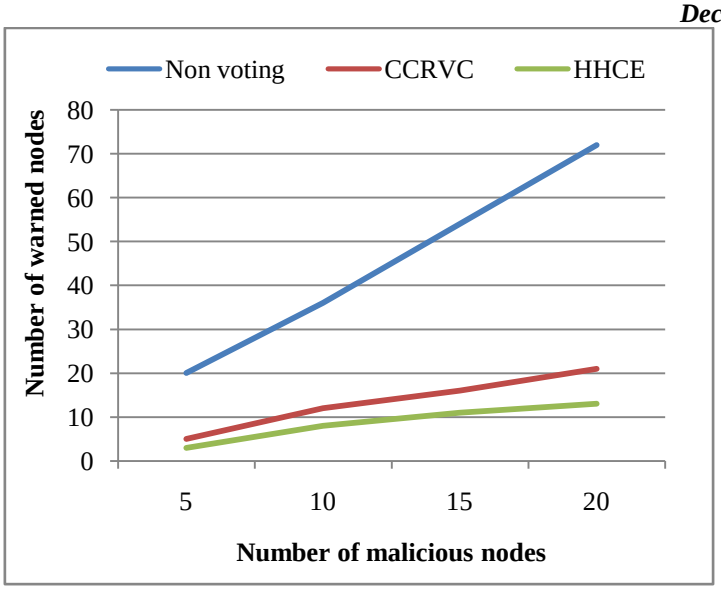

Fig. 4. The number of warned nodes in WL

In this graph measure the results of the proposed HHCE schema and existing CCRVC, Nonvoting schema based on the malicious nodes vs number of warned nodes in the network. It is clearly experimented that the number of warned nodes becomes less in the proposed methods when compare to existing methods .It can observe with the intention of the total number of nodes in the WL is more or less equal to total number of malicious nodes in the network.

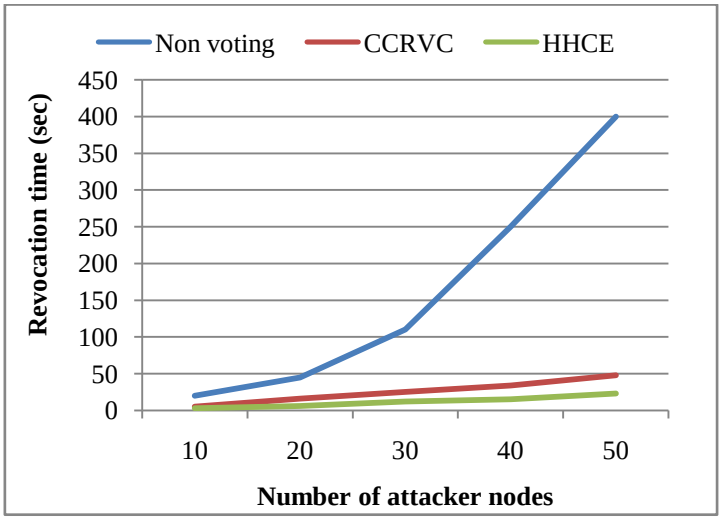

Fig. 5. Revocation time vs. methods

In this graph measure the results of the proposed HHCE schema and existing CCRVC, Nonvoting schema based on the number of attacker nodes vs revocation time in the network. It is clearly experimented that the number of attacker nodes the revocation time taken to complete the process becomes less when compare to existing methods .It can observe that if the total number of attacker nodes increases the revocation time of the proposed HHCE schema is less when compare to existing methods.

V. CONCLUSION AND FUTURE WORK

In this paper, majorly study the problem of the secure communications in MANET based on the creation of certificate revocation of attacker nodes. In this paper proposed a hybrid cubes certificate encryption revocation scheme come together through the qualities to revoke malicious certificate and solves the security problem. The scheme can revoke an indict node based on a single node's accusation, as compared to the voting-based mechanism. In addition to invalidate a malicious attacker's certificate three major important stages are followed in this work, these stages are accusing, verifying, and notifying, thus improving the accuracy as compared to the conventional methods such as non-voting based mechanism, CCRVC scheme. Particularly, proposed HCCE discharge and re-establish the reasonable nodes, and to progress the number of presented normal nodes in the MANET. It shows that the proposed certificate revocation scheme is successful and well-organized to assurance secure communications in mobile ad hoc networks. Our future work motivation incorporates a better programming concept for attacks. Then determination develops a scripting language move toward, where attack development can be articulated in a structure with the intention of is straightforwardly reasonable through individual and executable through machine.

REFERENCES

[1] Y. Huang and W. Lee, Attack analysis and detection for ad hoc routing protocols. *In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04),* French Riviera, France, 2004.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Comm.,* vol. 11, no. 1, pp. 38-47, 2004.

[3] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," *IEEE Wireless Comm., vol*. 14, no. 5, pp. 8-20, 2007.

[4] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," *IEEE Comm. Surveys and Tutorials,* vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[5] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," *IEEE Trans. Dependable and Secure Computing,* vol. 2, no. 3, pp. 233-247, 2005.

[6] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," *IEEE Trans. Vehicular Technology*, vol. 58, no. 5, pp. 2471-2481, 2009.

[7] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," *IEEE Wireless Comm. Magazine*, vol. 14, no. 5, pp. 85-91, 2007.

[8] J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," *ACMSIGOPS Operating Systems Rev*., vol. 40, no. 3, pp. 18-21, 2006.

[9] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," *Proc. IEEE 71st Vehicular Technology Conf. (VTC '10),* 2010.

[10] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Trans. Networking*, vol. 12, no. 6, pp. 1049-1063, 2004

[11] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate evocation Scheme for Mobile Ad Hoc Networks," *Ad Hoc Network,* vol. 6, no. 1, pp. 17-31, 2008.

[12] J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, 2006.

[13] J. H. Cho, A. Swami and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", I*EEE Communications Surveys & Tutorials*, (2011), pp. 562-583.

[14] J. Duan, Y. Qin, S. Zhang, T. Zheng and H. Zhang, "Issues of Trust Management for Mobile Wireless Sensor Networks", *7th International Conference on Wireless Communications*, Networking and Mobile Computing, (2011), pp. 1-4.

[15] S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad-Hoc Networks", *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, (2008), pp. 3-9.

[16] Shen, J. Jin, X. & Zhou, C. (2005).: A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation, PCM 2005, *Part II, LNCS 3768* pp. 270-280.

[17] Li, C. Li, S. Chen, G. & Halang, W. A. (2008) Cryptanalysis of an Image Encryption Scheme Based on a Compound Chaotic Sequence, *Image and Vision Computing*.

[18] Granboulan, L. Levieil E. & Piret G. (2006) Pseudorandom Permutation Families over Abelian Groups. *In Fast Software Encryption 2006*, volume 4047 of LNCS, pp 57-77. Springer-Verlag.

[19] Scalable Network Technologies: Qualnet, http://www.scalablenetworks. com, 2012

